



IBM Systems - iSeries

Управление системой
Обеспечение ГОТОВНОСТИ

Версия 5, выпуск 4





IBM Systems - iSeries

Управление системой
Обеспечение готовности

Версия 5, выпуск 4

Примечание

Перед началом работы с этой информацией и с описанным в ней продуктом ознакомьтесь с разделом “Примечания”, на стр. 23.

Издание четвертое (февраль 2006 года)

Это издание относится к версии 5, выпуску 4, модификации 0 продукта IBM i5/OS (код продукта 5722-SS1), а также ко всем последующим выпускам и модификациям, если в новых изданиях не будет указано обратное. Данная версия работает не на всех моделях систем с сокращенным набором команд (RISC) и не работает на моделях с полным набором команд (CISC).

© Copyright International Business Machines Corporation 1998, 2006. Все права защищены.

Содержание

Руководство по обеспечению

готовности 1

Новое в V5R4 1

Концепции обеспечения готовности 1

Цена готовности 3

Выбор оптимального уровня готовности 3

Предупреждение незапланированного простоя 5

 Подготовка к возможному сбою диска 5

 Действия при сбое питания 7

 Эффективное управление системой 8

 Подготовка пространства для сервера 9

Сокращение времени незапланированного простоя 9

 Сокращение времени незапланированного простоя 9

 Восстановление последних изменений после

 незапланированного выключения 10

 Восстановление данных после незапланированного

 выключения 11

 Сокращение времени изменения независимого
 пула дисков 12

Сокращение времени запланированного простоя 13

 Сокращение времени резервного копирования 13

 Сокращение времени на обслуживание и

 обновление программного обеспечения 15

 Сокращение времени на обслуживание и

 обновление аппаратного обеспечения 16

Готовность нескольких систем: кластеры 16

Решения для обеспечения устойчивости данных для

кластеров i5/OS 17

Информация, относящаяся к обеспечению готовности 20

Приложение. Примечания 23

Товарные знаки 25

Условия 25

Руководство по обеспечению готовности

С появлением сети Internet проблема постоянного доступа к данным и приложениям компаний приобрела особое значение. Если потенциальный клиент не сможет открыть ваш Web-сайт просто потому, что ваша система отключена, он наверняка обратится к одному из ваших конкурентов.

Коэффициент готовности указывает, с какой вероятностью данные и приложения будут доступны для работы, когда вы обратитесь к ним. У разных компаний есть разные требования к готовности. Различные системы и приложения в пределах одной компании также могут предъявлять разные требования к готовности. Этот раздел призван помочь вам разобраться в вопросах готовности серверов iSeries и помочь выбрать правильные средства ее обеспечения. Очень важно понимать, что обеспечение высокой готовности невозможно без тщательного планирования, а все средства и инструменты принесут пользу только в том случае, если вы воспользуетесь ими до возникновения сбоя.

Перед началом планирования обеспечения готовности системы следует изучить основные понятия готовности, осознать стоимость и риск, связанные с простоями, и определить, какой уровень готовности необходим вашей компании. После того, как вы разберетесь с основными понятиями, связанными с готовностью, и определите требования к уровню готовности для своей организации, можно начинать планирование действий, необходимых для поддержания этого уровня.

Новое в V5R4

В этом разделе приводится информация о новой функции, относящейся к обеспечению готовности.

Дополнения в информации об обеспечении готовности

В данном выпуске в эту информацию внесено несколько обновлений. Включены следующие разделы:

- Описание новых функций работы с пулом дисков, таких как IOP вспомогательного кэша и RAID
- Новая информация о технологиях восстановления данных
- Новая информация о сохранении из второй копии данных
- Изменения в последней информации об уменьшении времени сохранения, SMAPP и о ведении журнала

Концепции обеспечения готовности

Прежде чем начать планирование обеспечения готовности системы, вам следует ознакомиться с некоторыми ключевыми концепциями.

Для предприятий и поддерживающие их работу ИТ-операции следует определить, какие решения и технологии отвечают их требованиям. При соблюдении требований непрерывности работы предприятия эта задача становится достаточно сложной. Следует разработать и задокументировать подробные требования к непрерывности работы, определить типы решений и оценить выбранные решения. Это довольно сложная задача.

Непрерывность бизнеса - это способность выдерживать простои, то есть промежутки времени, в течение которых система недоступна, а также выполнять важные операции в обычном режиме без прерывания в соответствии с определенными соглашениями об уровне обслуживания. Для достижения требуемого уровня непрерывности бизнеса следует выбрать набор служб, программного и аппаратного обеспечения и процедур, задокументировать выбранные элементы, развернуть их и применять на регулярной основе. Решение для обеспечения непрерывности бизнеса должно охватывать данные, операционную среду, приложения, среду, управляющую приложениями, и конечный пользовательский интерфейс. Все эти элементы должны быть доступны для реализации законченного решения обеспечения непрерывности бизнеса. План обеспечения непрерывности бизнеса включает восстановление после аварии (DR) и высокую готовность (HA).

Восстановление после аварии (DR) представляет план мероприятий в случае простоя всего производства, например, в случае стихийного бедствия. DR может включать набор ресурсов, планов, служб и процедур для восстановления важных приложений и возобновления нормальной работы из удаленного офиса. *План восстановления после аварии* включает утвержденную цель восстановления после аварии (например, восстановить работу в течение восьми часов) и указывает на приемлемые уровни снижения производительности.

Еще одним важным аспектом обеспечения непрерывности бизнеса для многих заказчиков является *высокая готовность*, то есть способность выдерживать простои (запланированные, незапланированные и аварии) и обеспечивать непрерывное выполнение всех важных приложений. Основной задачей является уменьшение времени простоя до менее чем 0,001% общего служебного времени. Различия между высокой готовностью и восстановлением после аварии обычно заключаются в более высоких требованиях к времени восстановления (секунды и минуты) и месту проведения восстановления (работа конечного пользователя не прерывается).

Параметром степени готовности является время *простоя*, то есть периода времени, когда система недоступна для пользователей. Во время *запланированного простоя* вы умышленно делаете систему недоступной для пользователей. В это время вы можете запустить необходимые пакетные задания, создать резервную копию сервера или применить исправления.

Время резервного копирования - это период времени, когда система будет недоступна для пользователей из-за выполнения резервного копирования. Обычно резервное копирование выполняют ночью или в выходные, когда нагрузка на систему минимальна.

Незапланированный простой (называемый также неожиданным простоем) обычно бывает вызван сбоем в системе. При адекватной стратегии резервного копирования, после многих сбоев (таких как сбой диска, сбой питания, сбой программы или ошибка пользователя) систему удастся восстановить. Однако если сбой был вызван полной потерей системы, например, в результате торнадо или цунами, восстановление будет возможно только в случае, если вы точно следовали предварительно разработанному плану восстановления.

Решения для обеспечения высокой готовности предоставляют полностью автоматизированный автоматический перенос ресурсов в резервную систему для обеспечения непрерывной работы конечных пользователей и приложений. Эти решения должны предоставить точку немедленного восстановления и обеспечить меньшее время восстановления по сравнению с другими решениями.

В отличие от восстановления после аварии, применяемом при простое всей системы, решения для обеспечения высокой готовности можно настроить для отдельных важнейших ресурсов системы, например для конкретного экземпляра приложения. В системе i5/OS решения для обеспечения высокой готовности основаны на применении кластерной технологии. Кластеры i5/OS можно применять для того, чтобы избежать негативного влияния как запланированных, так и незапланированных простоев. Даже в случае простоя сервера нормальная работа предприятия не будет нарушена. *Кластер* - это набор взаимосвязанных сложных систем, работа с которыми ведется как с единым ресурсом. Применение кластера обеспечивает скоординированный, распределенный по системам процесс выполнения решения. Результатом является более высокая степень готовности, некоторое горизонтальное расширение предприятия и более простое администрирование. Законченное решение, кроме механизмов обеспечения устойчивости данных, должно охватывать операционную среду, среду, управляющую приложениями, устойчивость приложений и конечный пользовательский интерфейс. Работа кластеров сосредоточена на всех аспектах законченного решения. Встроенные службы ресурсов кластеров позволяют определить кластер систем и набор ресурсов, которые следует защитить в случае простоя. Службы ресурсов кластеров обнаруживают наличие простоя и координируют автоматический перенос важнейших ресурсов в резервную систему.

Цена готовности

Трудно не согласиться с тем, что доступность сервера исключительно важна. Однако мало кто может правильно оценить, например, границу стоимости дополнительного программного обеспечения, необходимого для поддержания повышенного коэффициента готовности.

Приведенные ниже инструкции помогут вам оценить стоимость оказываемых вами информационных услуг:

1. **Составьте список основных служб и решений, реализованных в вашей системе.** Система построена таким образом, чтобы пользователи и решения могли выполнять важные для бизнеса задачи. Система предоставляет решения для выполнения функций предприятия. Если система недоступна, функции предприятия либо не могут быть выполнены, либо ухудшаются в значительной степени, вызывая снижение дохода предприятия либо рост расходов.
2. **Оцените издержки, вызванные недоступностью перечисленных вами служб.** Каждое приложение или служба оказывают непосредственное влияние на работу предприятия. Необходимо оценить это влияние и определить суммарную стоимость для вашего предприятия.
3. **Оцените прямые и косвенные издержки.** Прямые издержки - это издержки, непосредственно вызванные простоем системы. Косвенные издержки - это, например, издержки других отделов или служб, возникшие в результате недоступности сервера.
4. **Оцените материальные и нематериальные издержки.** Материальные издержки - это издержки, которые можно оценить в денежном выражении. Однако есть и другие издержки, которые невозможно измерить деньгами, например, доля рынка, упущенная возможность или хорошее отношение заказчиков.
5. **Проанализируйте фиксированные и переменные издержки.** Фиксированные издержки - это издержки, вызванные простоем, и не зависящие от его продолжительности. Переменные издержки - это издержки, величина которых зависит от продолжительности простоя сервера.

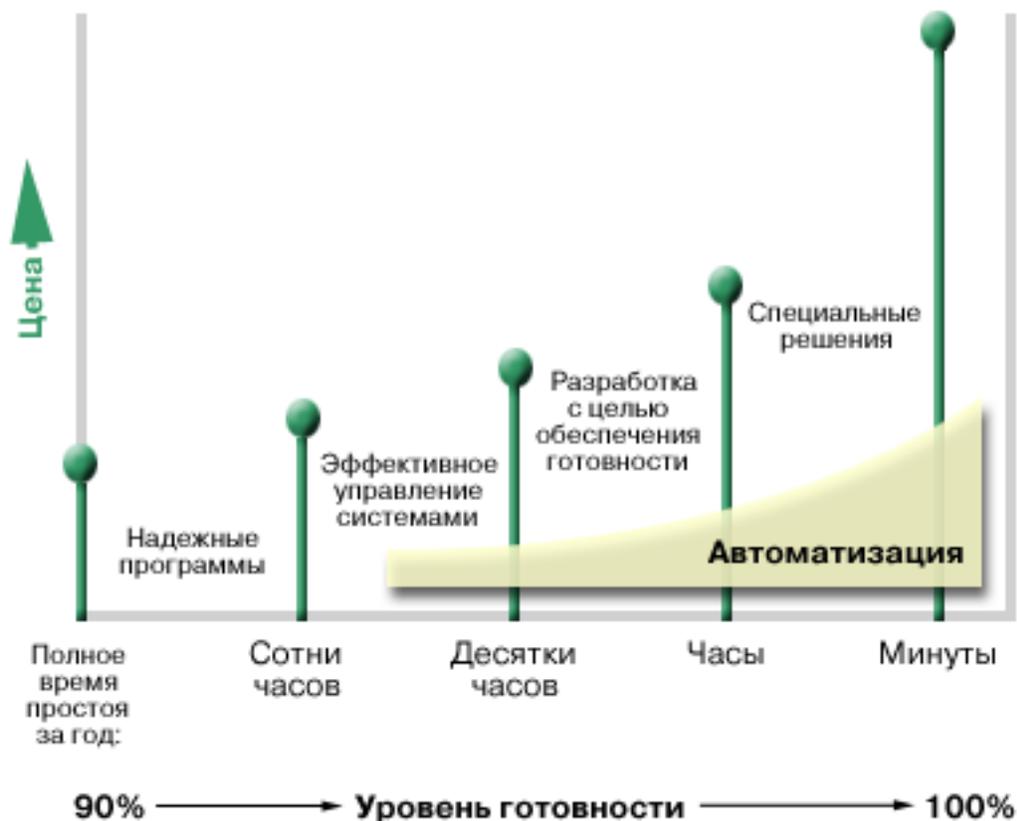
Выбор оптимального уровня готовности

Важно правильно оценить требования к готовности вашего предприятия. Реализация более высокого уровня готовности обходится дороже. Следует сопоставить потребности и службы с общей стоимостью реализации и обслуживания решений для обеспечения готовности.

Поэтому рекомендуется всесторонне оценить требования бизнеса и решить, на какой уровень готовности разумно потратить средства. При выборе оптимального уровня готовности учтите следующее:

Есть ли у вас приложения, требующие 100% готовности?

В большинстве случаев высокого уровня готовности можно добиться путем реализации рациональных процессов и методик управления системой. Чем ближе уровень готовности к постоянному, тем большие инвестиции вам потребуются. Перед тем, как делать такие инвестиции, тщательно оцените, нужен ли вам такой уровень готовности. На следующем рисунке показано, как различные технологии позволяют повысить готовность системы, но, в то же время, увеличивают ее стоимость.



Если требования к уровню готовности возрастают, можно рассмотреть применение решений для обеспечения готовности нескольких систем, например, кластеров.

Каково допустимое время простоя?

Полезно знать, какое время простоя подразумевается каждым уровнем готовности. В следующей таблице показано время простоя, соответствующее каждому уровню готовности:

Уровень готовности	Время простоя (в год)
90%	36,5 дней
95%	18,25 дней
99%	3,65 дней
99,9%	8,76 часов
99,99%	50 минут
99,999%	5 минут

Помимо того, какое время простоя допустимо для вашего сервера, необходимо также знать, в какой форме он может возникнуть. Например, готовность 99% может быть достаточной в том случае, если время простоя системы будет равномерно распределено по всему году. Однако те же самые 99% могут быть совершенно недопустимы в случае, если сервер будет недоступен всего один раз, но в течение 3 дней.

Также следует решить, в каких случаях время простоя приемлемо, а в каких - нет. Например, среднее время простоя в год в среднем составляет 9 часов. Если простой возникает в важные часы работы предприятия, он может оказать неблагоприятное воздействие на итоговый доход компании.

Какой уровень доступа необходим вашим клиентам?

- | Во времена, когда деловая активность велась только с 9 утра до 5 вечера, вы могли предоставлять клиентам и деловым партнерам доступ к серверу только в этот период времени. Однако с появлением Internet ситуация изменилась: теперь клиенты и деловые партнеры могут захотеть воспользоваться данными вашей компании в любое время дня и ночи. Ваши рабочие часы и даже дни могут отличаться от рабочих часов и дней ваших клиентов и деловых партнеров. При оценке требуемого уровня готовности следует выяснить, какой режим работы ожидают ваши клиенты от корпоративного сервера.

Предупреждение незапланированного простоя

Одним из способов повышения готовности системы является сокращение времени незапланированного простоя. Эти средства позволяют добиться минимального простоя при сбое системы.

Примечание: Если требуемого уровня готовности нельзя добиться с помощью одной системы, то рассмотрите возможность применения кластеров.

Подготовка к возможному сбою диска

Так как данные распределены по нескольким дискам, механизм защиты от сбоя дисков необходимо продумать заранее. Защита данных обеспечивает средства для обеспечения готовности данных, хранящихся на диске.

Дисковые накопители могут быть частью системы iSeries или могут быть подключены к ней внешне. Дисковые накопители в совокупности с оперативной памятью рассматриваются системой как единое пространство памяти. При сохранении файла вы не можете указать его расположение - система самостоятельно выбирает для него место, обеспечивающее наилучшую производительность. Во многих случаях данные файла могут быть распределены по нескольким дисковым накопителям. При добавлении в файл новых записей система выделяет для них дополнительное пространство на диске. Такой способ адресации называется *одноуровневой памятью*.

- | В дополнение к внутреннему дисковому накопителю также можно использовать IBM TotalStorage Enterprise Storage Server (ESS) для подключения внешних накопителей. ESS обеспечивает улучшенную защиту данных, возможность быстрого и эффективного копирования данных на другие серверы ESS, а также передачу одних и тех же данных по нескольким путям для избежания сбоев связи. Дополнительная информация о IBM TotalStorage Enterprise Storage Server (ESS) и его функциях приведена на странице Enterprise disk storage.

Защита устройств с проверкой четности

- | Защита с проверкой четности позволяет продолжить работу с системой после сбоя или повреждения диска. При этом дисковый адаптер ввода-вывода (IOA) подсчитывает и сохраняет значение четности для каждого бита данных. IOA подсчитывает значение четности на основании данных, расположенных в одинаковых позициях на разных дисках. При сбое одного диска данные с него можно восстановить с помощью значений четности и данных с других дисков. При восстановлении данных система продолжает работать.

- | Обзор защиты устройств с проверкой четности приведен на странице Device parity protection.

- | В системе i5/OS поддерживается два типа защиты устройств с проверкой четности:

RAID 5

- | При применении RAID 5 работа системы может быть продолжена в случае сбоя одного из дисков в наборе устройств с проверкой четности. В случае сбоя нескольких дисков данные будут потеряны и потребуются восстановление данных всей системы (либо только поврежденного пула дисков) с носителя резервной копии. В наборе устройств с проверкой четности, содержащем от 3 до 18 дисков, емкость одного из дисковых накопителей выделяется для хранения контрольных данных.

| RAID 6

| При применении RAID 6 работа системы может быть продолжена в случае сбоя одного или двух дисков в наборе устройств с проверкой четности. В случае сбоя более двух дисков потребуется восстановление данных всей системы (либо только поврежденного пула дисков) с носителя резервной копии. В наборе устройств с проверкой четности, содержащем от 4 до 18 дисков, для хранения контрольных данных выделяется емкость двух дисковых накопителей.

| Детальное сравнение RAID 5 и RAID 6 приведено в разделе Элементы защиты устройств с проверкой четности.

| Кэш записи и вспомогательный кэш записи IOA

| При отправке операции записи данные сначала записываются в кэш записи IOA диска, а затем - на диск. В случае сбоя IOA данные в кэше могут быть утеряны, что вызовет длительный простой системы и необходимость ее восстановления.

| Вспомогательный кэш записи представляет собой дополнительный IOA, идентичный IOA диска. Вспомогательный кэш записи обеспечивает защиту от длительных простоев вследствие сбоя IOA диска либо его кэша, предоставляя копию кэша записи, который можно восстановить после устранения неполадки IOA диска. Это предотвращает перезагрузку системы и возвращает систему в рабочее состояние сразу после замены IOA диска и завершения процедуры восстановления. Однако вспомогательный кэш записи не является устройством автоматического переноса ресурсов и не может поддерживать систему в рабочем состоянии в случае сбоя IOA диска или его кэша.

| Подробная информация о IOA кэша записи и вспомогательного кэша записи приведена в разделе Управление дисками на странице Write cache and auxiliary write cache IOA.

Зеркальная защита

Зеркальная защита данных рекомендуется для обеспечения наивысшей степени готовности системы и максимальной защиты от сбоев дисков. Защита обеспечивается путем хранения копии данных на другом диске. При сбое диска система продолжает работать, пользуясь данными с его зеркальной копии.

| В зависимости от аппаратного обеспечения, доступны следующие уровни зеркальной защиты: Уровень зеркальной защиты определяет, следует ли поддерживать рабочее состояние системы при сбоях на различных уровнях аппаратного обеспечения. Описание этих различных уровней защиты приведена в разделе Определение уровня защиты.

| Можно дублировать следующее относящееся к дискам аппаратное обеспечение:

- Дисковые накопители
- Дисковые контроллеры
- Шины ввода-вывода
- Адаптеры ввода-вывода
- Процессоры ввода-вывода
- Шины
- Корпусы расширения
- Кольцо HSL

Более подробная информация о зеркальной защите приведена в разделе Зеркальная защита.

Независимые пулы дисков

Независимые пулы дисков позволяют изолировать пользовательские данные от остальной системы. При сбое одного независимого пула дисков система продолжает работать с данными из других пулов дисков. В сочетании с различными уровнями защиты данных независимые пулы дисков предоставляют более широкие возможности для контроля ситуации при сбое дисков, а также лучшие методики предотвращения сбоев и восстановления системы. Более подробная информация приведена в разделе Независимые пулы дисков.

Географическая зеркальная защита

Географическая представляет собой функцию, которая позволяет хранить две идентичные копии независимого пула дисков на двух сайтах с целью обеспечения высокой готовности и восстановления после аварии. Копия в первичном узле является рабочей копией, а копия в резервном узле на другом сайте - зеркальной копией. Пользователи и приложения получают доступ к независимому пулу данных в первичном узле, в котором размещена рабочая копия. Географическая зеркальная защита представляет собой подфункцию распределенной по сайтам зеркальной защиты (XSM), которая является частью опции 41 системы i5/OS, High Available Switchable Resources.

Более подробная информация о географической зеркальной защите приведена в разделе Географическая зеркальная защита.

Альтернативные подключения дисковых накопителей

Можно указать до восьми подключений от каждого LUN (логического накопителя), созданного на сервере IBM TotalStorage Enterprise Storage Server (ESS), к IOP на сервере iSeries. Если применяется решение ESS, назначение альтернативных путей для одних и тех же данных позволяет осуществлять доступ к данным даже в случае сбоя какого-либо из подключений. Каждое из альтернативных подключений дискового накопителя является независимым. Наличие нескольких подключений обеспечивает готовность, допуская работу с дисковой памятью даже в случае сбоя одного из подключений.

Более подробная информация приведена в разделе Замечания об альтернативных подключениях дисковых накопителей.

Действия при сбое питания

Для того чтобы гарантировать, что система будет доступна всегда, когда потребуется, необходимо во-первых обеспечить ее бесперебойное питание, а во-вторых, защитить на случай сбоя питания.

Требования к питанию

Одним из этапов планирования конфигурации вашей системы является обеспечение ее бесперебойного питания. Необходимо выяснить все требования к электрической сети, кабелям питания, штепсельным вилкам и щитам питания а затем с помощью квалифицированного электрика обеспечить питание системы. Сведения о том, как проверить правильность источника питания сервера, приведены в разделе Определение требований к питанию.

Резервные источники питания

Некоторые системы IBM содержат резервные источники питания. Резервный источник обеспечивает питание системы в случае, когда стандартный источник питания выключается.

В некоторых системах поддерживается функция двухлинейного кабеля. Это позволяет обеспечивать питание системы от двух различных внешних источников питания. Это предотвращает незапланированные простои, связанные со сбоями источника питания.

Источники бесперебойного питания

Даже в случае принятия всех мер по обеспечению питания сервера, напряжение в сети может иногда пропадать, например, в случае урагана или наводнения. Для того чтобы исключить сбой системы при выключении питания, необходимо приобрести специальные устройства, обеспечивающие бесперебойное питание сервера. Одним из таких устройств является *источник бесперебойного питания (UPS)*. UPS может обеспечивать питанием процессор, диски, системную консоль и любые другие жизненно необходимые устройства. Источники бесперебойного питания имеют следующие преимущества:

- Они позволяют нормально работать при кратковременном отключении питания
- Они защищают систему от скачков напряжения
- Они позволяют завершить работу в обычном режиме, что сократит время восстановления при перезапуске сервера. Информация о разработке программ, управляющих выключением сервера в таких условиях, приведена в разделе Управление выключением сервера с помощью программы управления питанием.

Сведения об источниках бесперебойного питания для вашего сервера приведены в разделе Системы с бесперебойными источниками питания.

Генератор электроэнергии

Если в вашем здании возможны долговременные отключения электроэнергии, то может иметь смысл приобретение генератора. Генератор выгодно отличается от UPS тем, что обеспечивает питание даже при долговременном отключении электроэнергии.

Эффективное управление системой

Один из самых простых способов предотвратить незапланированный простой системы - это сделать все возможное для правильной и эффективной работы этой системы. Сюда входит выполнение профилактического обслуживания и задач управления системой, обеспечивающих надежную работу при пиковой нагрузке.

Большинство задач управления сервером можно автоматизировать, избежав тем самым потенциальных сбоев, вызванных ошибкой или недосмотром оператора.

Для обеспечения постоянной готовности можно контролировать работу системы и быстро реагировать на все возникающие неполадки. Для контроля и сбора данных о производительности сервера можно применять службы сбора информации и функции мониторов, входящие в состав Централизованного управления. Вы можете получать уведомления о всех неполадках, которые потенциально могут привести к простоям системы, и своевременно реагировать на них. Более подробная информация о планировании и контроле производительности сервера приведена в разделе Производительность.

Еще один важный компонент управления системами - это своевременная установка исправлений. При обнаружении неполадки в какой-либо программе iSeries, IBM выпускает для этой неполадки **исправление**, (называемое также временным исправлением программы или PTF). Для правильной и эффективной работы системы необходимо отслеживать выход новых исправлений и устанавливать их. Нужно разработать стратегию управления исправлениями и включить проверку и установку исправлений в стандартную процедуру обслуживания сервера. Более подробная информация о получении и применении исправлений приведена в разделе Работа с исправлениями. Разработать стратегию профилактического обслуживания системы iSeries в зависимости от конкретной среды и применяемых приложений, вам поможет Web-страница

Fix Maintenance Advisor .

- | Кроме этого, следует разработать стратегию добавления новых приложений к вашим системам. Перед установкой нового приложения или обновлением существующего следует убедиться, что имеются все необходимые элементы аппаратного и программного обеспечения. Важно также спланировать и протестировать эти новые или измененные приложения перед их внедрением в рабочую среду, чтобы избежать возможных простоев либо других нежелательных воздействий.

Подготовка пространства для сервера

Одним из средств повышения готовности является расположение системы в месте, удовлетворяющем специальным требованиям. На работу системы влияют несколько физических факторов.

Прежде всего, вам следует ознакомиться с сервером. Различные системы предъявляют различные требования к окружающей среде, поэтому с конфигурацией системы необходимо ознакомиться заранее. Подробная информация о параметрах моделей приведена в разделе Спецификации серверов. Подробная информация о физических параметрах подключаемого к серверу оборудования приведена в разделе Спецификация аппаратного обеспечения.

После ознакомления с физическими параметрами сервера изучите следующие вопросы:

- **Расположение.** Физическое расположение сервера может повлиять на его доступность. Например, если доступ в помещение с системой открыт для всех, то кто-нибудь может ее случайно повредить или отключить кабель питания. Подробная информация о мерах предосторожности приведена в разделе Размещение сервера.
- **Кабели.** На кабели часто обращают мало внимания, однако без соответствующих кабелей система будет совершенно бесполезна. Все кабели должны находиться в хорошем состоянии и должны быть подключены правильно. Подробная информация о кабелях приведена в разделе Общие сведения о кабелях.
- **Окружающая среда.** Параметры окружающей среды сервера также играют существенную роль. В их число входит температура, влажность и другие факторы, которые могут повлиять на производительность сервера. Подробная информация о среде, в которой должен находиться сервер, приведена в разделе Размещение сайта: Окружающая среда, безопасность и защита.

Сокращение времени незапланированного простоя

Незапланированный сбой может произойти в любой момент, и вы должны быть готовы восстановить систему как можно быстрее.

Сервер должен оказаться в том состоянии, в котором он находился до выключения питания.

Если требуемого уровня готовности нельзя добиться с помощью одной системы, то рассмотрите возможность применения кластеров.

Сокращение времени незапланированного простоя

К сожалению, периодически случаются незапланированные простои системы. С помощью описанных в этом разделе инструментов обеспечения готовности можно максимально быстро перезапустить систему после такого простоя.

- | Перед выключением системой выполняется некоторый набор действий, позволяющий убедиться, что все данные согласованы, а задания завершены в управляемом режиме. При неожиданном сбое система не может выполнить эти действия. Данные инструменты следует применять совместно для ускорения запуска системы.

Подробные сведения об аварийном выключении системы приведены в разделе Включение и выключение системы.

В Отчете о реальных применениях уменьшения времени iSeries приведены сведения об управлении временем запуска сервера iSeries.

Системная защита путей доступа (SMAPP)

Путь доступа - это маршрут, по которому приложение считывает нужные записи в файле базы данных. С файлом может быть связано несколько путей доступа, если различным приложениям требуются записи в различной последовательности. При включении сервера после аварийного завершения система должна заново создать все пути доступа, что может занять достаточно много времени. SMAPP защищает пути

доступа, чтобы системе не пришлось создавать их при каждом включении. Это позволяет существенно сократить время восстановления после сбоя и вернуться к нормальной работе гораздо быстрее. Подробная информация о SMAPP, приведена в разделе Системная защита путей доступа.

Журналы путей доступа

Как и SMAPP, ведение журналов для путей доступа позволяет уменьшить время восстановления после аварийного выключения питания. Однако при использовании SMAPP система сама решает, решает, какие пути защищать. Поэтому если сервер сочтет важные для вас пути доступа некритическими, то время перезапуска может увеличиться. При применении журналов вы решаете, какие пути следует заносить в журнал.

Подробная информация о ведении журналов для путей доступа приведена в разделе SMAPP и журналы путей доступа.

- | SMAPP и журналы путей доступа можно применять отдельно. Однако если имеется возможность их совместного применения, можно максимально увеличить их эффективность при уменьшении времени запуска системы, поскольку все важные пути доступа оказываются защищенными.
- | Защита путей доступа важна также в том случае, если планируется применение служб копирования, связанных с дисками, например, распределенной по сайтам зеркальной защиты, или функций копирования IBM TotalStorage Enterprise Storage Solution (ESS), для того чтобы избежать реорганизации путей доступа при автоматическом переносе ресурсов на резервный сервер.

Независимые пулы дисков

При запуске или перезапуске системы можно отдельно включать каждый из независимых пулов дисков. Это позволяет запустить систему быстрее. Доступ к более важным данным можно обеспечить в первую очередь. В зависимости от приоритета данных можно изменять порядок независимых пулов дисков. Более подробная информация приведена в разделе Пример: Обеспечение доступа к независимому пулу дисков при запуске.

Восстановление последних изменений после незапланированного выключения

После внезапного выключения системы вашей задачей является как можно быстрее привести ее в нормальное рабочее состояние. Сервер нужно перевести в то состояние, в котором он находился до выключения питания, без ввода команд вручную.

При этом некоторые данные придется создать заново. Для этого предназначены некоторые специальные средства и утилиты.

Ведение журнала

Журнал позволяет сохранить информацию о транзакциях в случае его аварийного выключения. Система заносит в журнал информацию обо всех изменениях объекта. Подробное описание журналов приведено в разделе Управление журналами.

Управление фиксацией

Средства управления фиксацией позволяют обеспечить целостность данных в системе. Они позволяют обрабатывать группу изменений ресурсов, например, файлов баз данных или таблиц, как одну транзакцию. В результате в системе может быть выполнена либо вся группа изменений, либо ни одно из входящих в нее изменений. Предположим, что сбой питания произошел во время выполнения некоторой группы обновлений базы данных. Если средства управления фиксацией не применяются, то данные могут оказаться неполны или повреждены. В противном случае, все незавершенные операции не будут повторены при перезапуске компьютера.

Приложения, применяющие управление фиксацией, могут перезапустить приложение, если задание, группа активации или система были выключены аварийно. При этом вы будете уверены, что при перезапуске приложения в базе данных не будет частичных обновлений или незавершенных транзакций.

Подробное описание управления фиксацией приведено в разделе Управление фиксацией.

Восстановление данных после незапланированного выключения

В результате незапланированного сбоя, например, сбоя диска, данные в системе могут быть повреждены. Самым серьезным случаем является утрата всего оборудования, например, в результате стихийного бедствия.

Есть несколько способов предотвратить полную потерю данных или хотя бы свести объем таких данных к минимуму.

Резервное копирование и восстановление

Эффективная стратегия резервного копирования сервера жизненно необходима: время и средства, потраченные на создание и поддержание такой стратегии, будут с лихвой окуплены при необходимости восстановления данных. После создания стратегии ее необходимо всесторонне протестировать и убедиться, что данные сохраняются и восстанавливаются правильно. Стратегию резервного копирования следует обязательно перепроверять при любых изменениях в конфигурации системы.

Различные системы и бизнес-приложения требуют различных подходов, однако мы настоятельно рекомендуем вам делать полную резервную копию сервера не реже одного раза в неделю. Если вы работаете в динамичной среде, то сохранять измененные объекты следует чаще. Таким образом, если потребуются восстановить систему после сбоя, у вас всегда будет самая свежая копия данных.

Рекомендации по созданию стратегии резервного копирования и восстановления приведены в разделе Планирование стратегии резервного копирования. Инструкции по резервному копированию сервера приведены в разделе Резервное копирование сервера. Информация по восстановлению сервера приведена в разделе Восстановление сервера.

Одним из средств, призванных помочь вам при резервном копировании и восстановлении, является программа Backup, Recovery and Media Services (BRMS). BRMS помогает реализовать упорядоченную схему управления резервным копированием и восстановлением данных. Применение BRMS значительно упрощает и ускоряет выполнение самых важных и сложных процедур резервного копирования, включая интерактивное резервное копирование серверов Lotus. Кроме того, в случае аварии или сбоя системы возможно ее полное восстановление.

Помимо помощи при резервном копировании и восстановлении, BRMS позволяет хранить данные обо всех носителях с резервными копиями. Таким образом, вам не придется самостоятельно каталогизировать и упорядочивать носители с резервными копиями. BRMS также позволяет отслеживать перемещение носителей между различными зданиями вашей компании.

Более подробная информация о BRMS приведена в разделе Backup, Recovery and Media Services.

Полезная информация об управлении стратегией резервного копирования и восстановления приведена на Web-сайте IBM Business Continuity and Recovery Services .

Ограничение объема данных, которые могут быть потеряны

Вы можете сгруппировать дисковые накопители в наборы, называемые *дисковыми пулами*. Данные каждого дискового пула изолированы от других данных. В случае сбоя дискового накопителя вам потребуется восстановить только данные из того дискового пула, в который входил поврежденный диск.

Более подробная информация о пулах дисков, типах пулов, а также примеры использования пулов приведены в разделе Пулы дисков. Информация о настройке пулов дисков приведена в разделе Управление дисками.

Независимые дисковые пулы можно включать или выключать, не оказывая влияния на оставшуюся системную память. Такая операция возможна потому, что вся необходимая информация о дисковом пуле хранится в самом пуле. Независимые дисковые пулы имеют немало преимуществ как в односистемной, так и в многосистемной среде. Подробная информация приведена в разделе Независимые пулы дисков.

Логические разделы позволяют разделить одну систему на несколько независимых систем. Применение логических разделов - это еще один способ изоляции данных, приложений и других ресурсов. С помощью логических разделов можно увеличить производительность системы, например, запуская пакетные и интерактивные задания в разных разделах. Кроме того, данные можно защитить, установив критические приложения в отдельном логическом разделе. В таком случае сбой других программ не повлияет на работу критически важных приложений.

Более подробная информация о логических разделах приведена в разделе Логические разделы.

Сокращение времени изменения независимого пула дисков

В случае незапланированного простоя данные, хранящиеся в независимых пулах дисков, становятся недоступными до перезапуска. Для проведения быстрого и эффективного перезапуска следует применять рекомендованные стратегии включения независимых пулов дисков.

Эти стратегии представляют средства уменьшения времени включения независимых пулов дисков.

Синхронизация имени пользовательского профайла, UID, и GID

В среде кластеров предполагается, что пользовательские профайлы с одинаковым именем одинаковы на всех серверах. Имя является уникальным идентификатором в кластере. Однако в пользовательском профайле также содержится идентификатор пользователя (UID) и идентификатор группы (GID). Для уменьшения числа внутренних операций в процессе принудительного переноса ресурсов когда доступ к независимому пулу дисков прекращается на одном сервере и предоставляется на другом, следует синхронизировать значения UID и GID в домене восстановления для CRG устройства.

Применение рекомендованной структуры независимых пулов дисков

Рекомендуется размещать основную часть данных приложений в независимых пулах дисков и минимальное число непрограммных объектов - в SYSBAS, представляющей собой системный пул дисков и все настроенные базовые пулы. Системный пул дисков и базовые пользовательские пулы (SYSBAS) должны содержать первичные объекты операционной системы, библиотеки лицензионных программ и несколько пользовательских библиотек. Такая структура обеспечивает наилучшую защиту и производительность. Данные приложений изолированы от не связанных с ними сбоев и могут обрабатываться независимо от других операций в системе. Включение и принудительный перенос ресурсов оптимизированы для этой структуры.

Рекомендованная структура не исключает возможность других конфигураций. Например, можно начать с переноса небольшой части данных в группу пулов дисков и хранить основную массу данных в SYSBAS. Этот вариант также поддерживается. Однако следует ожидать более длительного времени включения и принудительного переноса ресурсов при использовании этой конфигурации, поскольку для объединения информации о перекрестных ссылках баз данных в группе пулов дисков требуется выполнение дополнительных операций.

Сокращение времени запланированного простоя

Запланированные периоды простоя необходимы и известны заранее, однако тот факт, что они запланированные, не означает, что они не нарушают работу компании. Чаще всего они связаны с обслуживанием системы.

- | Кластеры позволяют не замечать плановые простои, обеспечивая готовность приложений и данных в другой системе или разделе.

Сокращение времени резервного копирования

Сокращение времени резервного копирования позволяет также сократить время, в течение которого система недоступна.

Ключевым моментом любой стратегии резервного копирования является определение времени резервного копирования, то есть периода времени, в течение которого система будет недоступна для пользователей из-за выполнения резервного копирования. Требуется выполнить резервное копирование в пределах установленного промежутка времени. Для уменьшения влияния времени резервного копирования на доступность системы можно уменьшить это время одним из описанных ниже способов.

Улучшенные технологии записи на магнитную ленту

Применение технологий более быстрой и более плотной записи на магнитную ленту может уменьшить суммарное время резервного копирования. Дополнительная информация приведена в разделе Устройства внешней памяти.

Параллельные операции сохранения

Одновременное применение нескольких накопителей на магнитной ленте позволяет уменьшить время резервного копирования, увеличивая в несколько раз производительность по сравнению с применением одного устройства. Дополнительная информация приведена в разделе Выполнение сохранения на нескольких устройствах для уменьшения времени сохранения.

Сохранение на несъемных носителях

Сохранение на такие носители (например, непосредственно на дисковый накопитель) выполняется быстрее чем на съемные. Данные можно будет перенести на съемный носитель позже. Дополнительная информация приведена в разделе Сохранение на виртуальную магнитную ленту.

Параллельное резервное копирование

Можно уменьшить время резервного копирования, сохраняя объекты в то время, как они еще используются системой, либо выполняя оперативное резервное копирование.

| Сохранять активные объекты

- | Функция сохранения активных объектов представляет собой опцию, доступ к которой можно получить с помощью Backup, Recovery and Media Services (BRMS) и с помощью нескольких команд сохранения.
- | Сохранение активных объектов может значительно уменьшить время резервного копирования либо совсем его игнорировать. Это позволяет сохранять данные в системе в процессе работы приложений без необходимости помещения системы в состояние с ограничениями. Функция сохранения активных объектов создает контрольную точку данных во время проведения операции сохранения. Сохраняется версия данных на этот момент; при этом выполнение других операций не прерывается. Более подробная информация о сохранении активных объектов приведена в разделе Сохранение активного сервера.

Параллельное резервное копирование

Другим способом сохранения используемых в данный момент объектов является *параллельное резервное копирование*. Параллельное резервное копирование во многом похоже на сохранение активных объектов за тем исключением, что в нем не применяются контрольные точки. Это означает, что пользователи могут работать с объектами в течение всего процесса резервного копирования. Backup, Recovery, and Media Services (BRMS) поддерживает параллельное резервное копирование серверов Lotus, таких как Domino и QuickPlace. Результаты параллельного резервного копирования можно сохранять на магнитных лентах, в библиотеке магнитных лент, в файлах сохранения или на сервере Tivoli Storage Manager (TSM). Более подробная информация о параллельном резервном копировании серверов Lotus приведена в разделе Backup, Recovery and Media Services.

Примечание: Мы настоятельно рекомендуем вам продолжать сохранение системной информации даже при сохранении активных объектов и параллельном резервном копировании. Некоторую важную системную информацию нельзя сохранить при сохранении активных объектов и параллельном резервном копировании.

Резервное копирование из второй копии

Для уменьшения времени резервного копирования можно использовать несколько методик, связанных с резервным копированием из второй копии данных.

Примечание: При выполнении сохранения из второй копии следует убедиться в согласованности содержимого копий. Может потребоваться приостановка работы приложения.

Эти методики включают:

Сохранение из второй системы

С помощью некоторых технологий, например, репликации, можно сделать доступной вторую копию данных, что позволяет сдвинуть промежуток времени сохранения с первичной копии на вспомогательную. С помощью этой методики можно устранить время резервного копирования в первичной системе. Следовательно, резервное копирование не влияет на производительность этой системы, поскольку выполняется во вспомогательной системе.

IBM TotalStorage Enterprise Storage Server (ESS) FlashCopy, применяемый вместе с iSeries Copy Services для ESS toolkit

IBM TotalStorage Enterprise Storage Server (ESS) предоставляет расширенные возможности для работы с памятью. В этой технологии применяется функция ESS FlashCopy для независимого пула дисков. Отдельный сервер ESS создает синхронную версию независимого пула дисков, причем хост не участвует в создании копии. Этот инструментарий позволяет передать копию в резервную систему для выполнения операций сохранения или другой обработки. Информация о IBM TotalStorage (ESS) и его функциях размещена на web-сайте IBM TotalStorage.

Уменьшение объема сохраняемых данных

Можно сократить продолжительность запланированных простоев, сохраняя меньшее количество данных. Существует несколько способов разделения данных системы для этой операции.

Примечание: Можно использовать для резервного копирования программу Backup, Recovery and Media Services.

Дополняющее резервное копирование

Дополняющее резервное копирование позволяет сохранять только изменения объектов. Есть два типа дополняющего резервного копирования: совокупное и сохранение только изменений. *Аккумулирующее резервное копирование* - это резервное копирование всех измененных и новых объектов с момента проведения

последнего полного резервного копирования. При этом сохраняются все изменения объектов по отношению к полной резервной копии. Оно применяется в случаях, когда объекты изменяются редко или изменяются незначительно. При проведении *резервного копирования только изменений* включаются все измененные и новые объекты с момента проведения последнего полного или аккумулирующего резервного копирования.

Такой тип резервного копирования применяется в случаях, когда данные изменяются часто. Допустим, что вы выполняете полное резервное копирование каждую субботу. Некоторые библиотеки используются очень активно, поэтому сохранять их следует чаще одного раза в неделю. Для их сохранения можно выполнять дополняющее резервное копирование через день. Это позволит сократить время простоя, не жертвуя при этом полнотой резервных копий.

Данные защиты и конфигурации

Вы также можете сократить время простоя при резервном копировании, изолировав некоторые данные и сохраняя их отдельно. В число данных защиты входят пользовательские профили, списки прав доступа и владельцы прав доступа. Данные конфигурации описывают, как настроена система, включая описания линий, описания устройств, списки конфигурации и т.п. Данные этих типов сохраняются при полном резервном копировании, однако вы можете сохранить их отдельно, не выключая всю систему. Более подробная информация о сохранении этих данных приведена в разделе Сохранение частей сервера вручную.

Пропуск некоторых объектов

Время резервного копирования можно уменьшить, сократив число сохраняемых объектов или исключив повторное сохранение объектов. Для этого достаточно просто не выполнять сохранение некоторых объектов. Например, можно сохранять все пользовательские библиотеки, кроме временных. Это позволит сократить время, затрачиваемое на резервное копирование. Многие команды сохранения позволяют задать список пропускаемых объектов. Информация о таких командах приведена в разделах Команды сохранения различных частей сервера и Команды сохранения определенных типов данных. Кроме того, для исключения объектов из списка сохраняемых можно воспользоваться продуктом Backup, Recovery and Media Services.

Архивирование данных

Данные, которые не требуются для нормальной работы предприятия, можно заархивировать и поместить на внешнее хранение. Эти данные включаются в работу только при необходимости, возможно, в конце месяца или квартала. Ежедневное время резервного копирования уменьшается, поскольку при этом не сохраняются заархивированные данные.

Сокращение времени на обслуживание и обновление программного обеспечения

Поддерживать доступность системы позволяет эффективное планирование, управление исправлениями и установка новых выпусков.

Работа с исправлениями

Для сокращения времени простоя системы вам необходима эффективная стратегия управления исправлениями. Поддержание сервера на текущем уровне исправлений позволяет уменьшить число возникающих проблем. Обязательно следуйте при применении исправлений выбранной стратегии. Рекомендации по выбору такой стратегии приведены в разделе Планирование стратегии управления исправлениями.

Отдельные исправления могут быть **отложенными** или **немедленными**. Отложенные исправления можно загрузить и применить в два этапа. Их можно загрузить, не нарушая работу системы, а затем применять при следующем перезапуске. Немедленные исправления не требуют перезагрузки, что позволяет избежать простоя системы. Для применения немедленных исправлений могут потребоваться дополнительные шаги,

описанные в сопроводительном письме. Подробная информация о применении исправлений приведена в разделе Установка исправлений.

Установка нового выпуска

При установке новой версии i5/OS требуется перезагрузка системы. Для минимизации времени простоя, обновление программного обеспечения следует тщательно спланировать. Подробная информация о планировании обновлений приведена в разделе Обновление или замена системы i5/OS и связанного программного обеспечения.

Сокращение времени на обслуживание и обновление аппаратного обеспечения

Эффективное планирование обслуживания и обновления аппаратного обеспечения может значительно снизить или даже избежать негативного влияния этих действий на степень готовности сервера.

Иногда приходится выполнять обычное обслуживание аппаратного обеспечения или устанавливать более мощное оборудование. Эти операции могут прервать обычную работу системы.

Перед началом обновления системы все операции необходимо тщательно спланировать. Чем тщательнее вы спланируете конфигурацию нового сервера, тем быстрее его удастся обновить. Дополнительная информация о планировании приведена в разделе Обновления.

Оперативное обслуживание

Многие компоненты аппаратного обеспечения системы iSeries можно заменять, добавлять или удалять оперативно в процессе работы системы. Например, функция "оперативной замены" поддерживается для разъемов для плат PCI, дисковых накопителей и резервных вентиляторов и блоков питания. Оперативное обслуживание увеличивает готовность системы и позволяет проводить обновления, обслуживание и ремонт, не мешая работе пользователей системы.

Подробные сведения приведены в разделе Оперативное обслуживание.

Модернизация по запросу

Функция модернизации по запросу IBM eServer позволяет активировать дополнительные процессоры и, соответственно, платить за них только при необходимости. Таким образом, вычислительную мощность можно наращивать без прерывания обычной работы.

Модернизация по запросу - это функция iSeries, позволяющая активировать один или несколько центральных процессоров без прерывания работы. Минимальной добавляемой единицей является один процессор, а максимальное значение ограничено числом резервных процессоров в системе. Возможность увеличивать мощность по запросу имеет большое значение в системах, где прерывание работы недопустимо.

Дополнительная информация об этой функции приведена в разделе Модернизация по запросу.

Готовность нескольких систем: кластеры

В средах с несколькими системами можно применять кластеры в качестве стратегии поддержания высокой или непрерывной доступности систем и приложений.

Кластер - то группа систем, работающих вместе как один сервер. Если для работы вашей компании важна высокая готовность систем, то кластеры могут оказаться наилучшим решением.

Системы в кластере работают совместно, в одной вычислительной среде. В одном кластере могут работать до 128 систем. Это позволяет эффективно сгруппировать системы в пределах одной вычислительной среды с

практически 100-процентной доступностью критических приложений и данных. Таким образом, важные системы и приложения будут доступны всегда. Кроме того, кластеры позволяют упростить управление системами и повысить масштабируемость всей вычислительной среды вашего предприятия.

При принятии решения относительно того, стоит ли применять кластеры в вашей вычислительной среде, попробуйте соотнести стоимость кластера с издержками, возникающими при простое системы.

Применение кластеров в среде увеличивает доступность приложений. Уровень доступности приложений будет зависеть от степени интеграции приложений со службами ресурсов кластеров. Более подробная информация о таких приложениях приведена в разделе Программы с высокой доступностью.

Более подробная информация о кластерах приведена в разделе Кластеры. Более подробная информация о работе кластеров в сочетании с другими решениями, позволяющими повысить готовность системы, приведена в разделе High availability and clusters .

Программы с высокой доступностью

Приложения с высокой доступностью предоставляют пользователям постоянный доступ к данным и функциям приложения вне зависимости от запланированных или незапланированных простоев. В системе i5/OS представлена архитектура устойчивости приложений, которая поддерживает различные степени высокой доступности приложений. Приложения с самой высокой степенью доступности усилены интегрированными функциями и обеспечивают автоматизацию среды. Контроль этих функций осуществляется с помощью утилит управления кластерами. Более подробная информация по этим вопросам приведена в разделе Приложения для кластеров.

Промежуточное программное обеспечение для кластеров iSeries

- | Промежуточное программное обеспечение для кластеров iSeries представляет собой группу продуктов других фирм, которые предоставляют службы и функции копирования данных и управления кластерами.
- | Эти продукты работают с функциями Служб ресурсов для кластеров системы i5/OS и поддерживают архитектуру кластеров iSeries. Список промежуточного программного обеспечения для кластеров и описание критериев, которым эти программы должны соответствовать, приведены на странице High Availability and Clusters. 

Решения для обеспечения устойчивости данных для кластеров i5/OS

В этом разделе представлен обзор различных технологий обеспечения устойчивости данных, которые можно применять вместе с кластерами i5/OS для увеличения степени готовности в средах с несколькими системами.

Устойчивость данных - это способность данных оставаться доступными для приложений даже в случае сбоя в системе, которая владеет этими данными. Выбор набора технологий обеспечения устойчивости данных в соответствии с общей стратегией непрерывности работы предприятия может оказаться весьма сложным. Важно понимать особенности различных решений обеспечения устойчивости данных. Эти решения можно использовать либо отдельно, либо вместе с кластерами для увеличения готовности в средах с несколькими системами. По вашему усмотрению можно выбрать либо отдельное решение, либо их комбинацию.

Дополнительная информация приведена в разделе Решения для обеспечения устойчивости данных для кластеров высокой готовности IBM i5/OS. В разделе "Сравнительные характеристики" проводится подробное сравнение атрибутов этих технологий.

Репликация

С помощью репликации изменения объекта копируются в сохраненную копию практически в режиме реального времени. Репликация представляет собой одно из наиболее часто применяемых решений для обеспечения высокой готовности в средах с несколькими системами. В системах iSeries это решение чаще всего реализуется с помощью делового партнера.

Следует рассмотреть возможность применения репликации при соблюдении следующих условий:

- Необходимо иметь две или более копии данных.
- Необходим параллельный доступ ко второй копии данных.
- Необходимо уменьшить время резервного копирования.
- Необходима выборочная репликация объектов в библиотеке или каталоге.
- ИТ-персонал вашего предприятия может отслеживать состояние среды копирования.
- Необходима географическая рассредоточенность копий, особенно в том случае, если расстояние между ними превышает допустимое аппаратными средствами.
- Уже развернуто решение, в котором применяется логическая репликация объектов.
- Необходимо решение, не предъявляющее специальных требований к аппаратному обеспечению.
- Время восстановления после сбоя и принудительного переноса ресурсов не должно превышать десятков минут.
- Целостность на уровне транзакций важна для всех объектов с журналами.

Переносимые пулы дисков

Переносимые пулы дисков - это устройства для сохранения в операционной системе, независимые от отдельной системы. Это позволяет "переносить" пулы дисков из одной системы в другую без выполнения полной IPL. Основными преимуществами переносимых пулов дисков является простота и удобство обслуживания. Одна копия данных всегда является текущей без необходимости синхронизации с другими версиями, что снижает затраты на администрирование.

Следует рассмотреть возможность применения переносимых пулов дисков при соблюдении следующих условий:

- Только одна копия данных с аппаратной защитой удовлетворяет потребностям предприятия и необходимо принять меры, позволяющие избежать незапланированных простоев, возникающих при сбоях дисковой подсистемы.
- Требуется простое решение, имеющее низкую стоимость и низкие требования к обслуживанию.
- Не требуется восстановление после аварии (DR).
- Требуется компенсировать влияние только плановых простоев и определенных типов незапланированных простоев.
- Исходная и целевая системы находятся на одном сайте.
- Необходимо согласовать время восстановления после сбоя и время принудительного переноса ресурсов в пределах нескольких минут независимо от объема транзакций.
- Целостность на уровне транзакций важна для всех объектов.
- Требуется немедленная готовность всех изменений объектов без потери текущих данных.
- Объекты вне независимого пула дисков либо не требуется реплицировать, либо управление этими объектами происходит посредством иного механизма.
- Необходима среда с высочайшей производительностью.
- В среде предусмотрено несколько независимых баз данных, которые можно перемещать между системами.

Распределенная по сайтам зеркальная защита

Распределенная по сайтам зеркальная защита в сочетании с функцией географической зеркальной защиты позволяет зеркально отображать данные, находящиеся на дисках на сайтах, разделенных значительным расстоянием. Географическая зеркальная защита предоставляет возможность репликации изменений в рабочей копии независимого пула дисков в зеркальную копию этого пула. После записи данных в рабочую копию операционная система зеркально отразит данные на вторую копию независимого пула дисков в другой системе. При этом хранится несколько идентичных копий данных.

Следует рассмотреть возможность применения распределенной по сайтам зеркальной защиты в следующих случаях:

- Требуется создаваемая системой вторая копия данных (на уровне IASP).
- Требуется две копии данных, но параллельный доступ ко второй копии обеспечивать не надо.
- Желательны относительно низкая стоимость и простота обслуживания решения, однако также требуется обеспечить восстановление после аварии.
- Требуется географическое рассредоточение копий, однако расстояние между копиями не оказывает негативное влияние на параметры производительности предприятия.
- Необходимо согласовать время восстановления после сбоя и время принудительного переноса ресурсов в пределах нескольких минут независимо от объема транзакций.
- Целостность на уровне транзакций важна для всех объектов.
- Требуется немедленная готовность всех изменений объектов без потери текущих данных.
- Объекты вне независимого пула дисков либо не требуется реплицировать, либо управление этими объектами происходит посредством иного механизма.
- Отсутствие доступа ко второй копии в процессе синхронизации допускается текущим уровнем обслуживания.

IBM TotalStorage Enterprise Storage Server PPRC, применяемое вместе с iSeries Copy Services для ESS toolkit

Это решение включает репликацию данных на уровне контроллера памяти во вторую систему с помощью служб копирования IBM TotalStorage Enterprise Storage Server (ESS). Независимый пул дисков является основным элементом хранилища для функции копирования на удаленный равноправный сервер (PPRC). PPRC создает вторую копию независимого пула дисков на другом ESS. Этот инструментариум поставляется как часть служб копирования iSeries для ESS. Предоставляется набор функций для комбинирования служб кластеров PPRC, IASP и i5/OS с целью координации проведения принудительного переноса ресурсов и восстановления после сбоя в группе ресурсов кластера.

Это решение предоставляет функцию удаленного копирования и позволяет скоординировать операции переноса, что обеспечивает достаточно высокую устойчивость данных в процессе синхронной репликации. В этом решении можно разместить вторую копию в резервной системе без выполнения IPL. Восстановление загрузочного накопителя не производится. Также имеется возможность применять это решение совместно с другими функциями служб копирования, связанными с ESS, например, с FlashCopy, что дает дополнительные преимущества, например, уменьшение времени сохранения.

Применение копирования на удаленный равноправный сервер (PPRC) IBM TotalStorage Enterprise Storage Server (ESS) с IASP и Toolkit рекомендуется в следующих случаях:

- Необходимо решение для DR с применением хранилища, особенно при работе с несколькими платформами.
- Нет необходимости в полной готовности (HA), однако для критических данных приложений требуется обеспечить восстановление после аварии и запланированные простои.
- Необходимо согласовать время восстановления после сбоя и время принудительного переноса ресурсов в пределах нескольких минут независимо от объема транзакций.
- Требуется две копии данных, но параллельный доступ ко второй копии обеспечивать не надо.

- Требуется географическое рассредоточение копий, однако расстояние между копиями не оказывает негативное влияние на параметры производительности предприятия. Как альтернативный вариант можно применять глобальное зеркальное копирование на удаленный равноправный сервер (PPRC), известное как асинхронное PPRC.
- Целостность на уровне транзакций важна для всех объектов.
- Требуется готовность всех изменений объектов без потери текущих данных.

Информация, относящаяся к обеспечению готовности

Некоторые источники, относящиеся к к обеспечению готовности. Более подробная информация о высокой готовности, резервном копировании, кластерах и связанные разделы приведены в руководствах iSeries, IBM Redbooks (в формате PDF) и на Web-сайтах. Вы можете просмотреть или напечатать любой из документов в формате PDF.

Руководства

- Backup and Recovery 
- Backup, Recovery and Media Services for iSeries 

IBM Redbooks

- Data Resilience Solutions for IBM i5/OS High Availability Clusters 
- Clustering and IASPs for Higher Availability 
- Striving for Optimal Journal Performance on DB2 Universal Database for iSeries 
- High Availability on the AS/400 System: A System Manager's Guide 
- AS/400 Remote Journal Function for High Availability and Data Replication 
- The System Administrator's Companion to AS/400 Availability and Recovery 
- IBM eServer iSeries Independent ASPs: A Guide to Moving Applications to IASPs 
- Introduction to Storage Area Network, SAN 
- iSeries and Storage Area Networks 
- Domino 6 for iSeries Best Practices Guide 
- IBM WebSphere V5.1 Performance, Scalability, and High Availability 
- Microsoft Windows Server 2003 Integration with iSeries 
- Integrating Backup Recovery and Media Services and IBM Tivoli Storage Manager 
- Planning for IBM eserver i5 Data Protection with Auxiliary Write Cache Solutions 
- Independent ASP Performance Study on the IBM eServer iSeries Server 
- Improve Whole System Backups with the New Save-While-Active Function 
- Choosing the right backup strategy for Domino 6 for iSeries 

- Multipath for IBM iSeries 
- The LTO Ultrium Primer for IBM iSeries Customers 
- Seven Tiers of Disaster Recovery 

Web-сайты

- High Availability and Clusters 
- Backup, Recovery and Media Services 
- Capacity on Demand 
- IBM Business Continuity and Recovery Services 
- iSeries for Capacity Backup 
- Logical Partitioning 
- Storage Solutions 
- Implementing PeopleSoft EnterpriseOne ERP 8.0 Using an Independent Auxiliary Storage Pool 
- Performance Management 
- IBM TotalStorage 

Разделы справочной системы iSeries Information Center

- Резервное копирование и восстановление
- Кластеры
- Управление фиксацией
- Управление дисками
- Управление журналами
- Логические разделы
- Устройства внешней памяти

Отчеты о реальных применениях

- Резервное копирование интегрированной файловой системы
- Уменьшение времени iSeries IPL

Сохранение файлов в формате PDF

Для того чтобы сохранить документ PDF на рабочей станции для последующего просмотра и печати, выполните следующие действия:

1. Откройте документ PDF в окне браузера (для этого щелкните на приведенной выше ссылке).
2. Откройте меню **Файл**.
3. Выберите **Сохранить как...**
4. Откройте каталог, в котором следует сохранить документ PDF.
5. Нажмите кнопку **Сохранить**.

Загрузка Adobe Reader

Копию этой программы можно загрузить с Web-сайта Adobe (www.adobe.com/prodindex/acrobat/readstep.html)



Приложение. Примечания

Настоящая документация была разработана для продуктов и услуг, предлагаемых на территории США.

IBM может не предлагать продукты и услуги, упомянутые в этом документе, в других странах. Информацию о продуктах и услугах, предлагаемых в вашей стране, вы можете получить в местном представительстве IBM. Ссылка на продукт, программу или услугу IBM не означает, что может применяться только этот продукт, программа или услуга IBM. Вместо них можно использовать любые другие функционально эквивалентные продукты, программы или услуги, не нарушающие прав IBM на интеллектуальную собственность. Однако в этом случае ответственность за проверку работы этих продуктов, программ и услуг возлагается на пользователя.

IBM могут принадлежать патенты или заявки на патенты, относящиеся к материалам этого документа. Предоставление вам настоящего документа не означает предоставления каких-либо лицензий на эти патенты. Запросы на приобретение лицензий можно отправлять по следующему адресу:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Запросы на лицензии, связанные с информацией DBCS, следует направлять в отдел интеллектуальной собственности в местном представительстве IBM или в письменном виде по следующему адресу:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

Следующий абзац не относится к Великобритании, а также к другим странам, в которых это заявление противоречит местному законодательству: ФИРМА INTERNATIONAL BUSINESS MACHINES CORPORATION ПРЕДОСТАВЛЯЕТ НАСТОЯЩУЮ ПУБЛИКАЦИЮ НА УСЛОВИЯХ “КАК ЕСТЬ”, БЕЗ КАКИХ-ЛИБО ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ, НЕЯВНЫЕ ГАРАНТИИ СОБЛЮДЕНИЯ ПРАВ, КОММЕРЧЕСКОЙ ЦЕННОСТИ И ПРИГОДНОСТИ ДЛЯ КАКОЙ-ЛИБО ЦЕЛИ. В некоторых странах запрещается отказ от каких-либо явных и подразумеваемых гарантий при заключении определенных договоров, поэтому данное заявление может не действовать в вашем случае.

В данной публикации могут встретиться технические неточности и типографские опечатки. В информацию периодически вносятся изменения, которые будут учтены во всех последующих изданиях настоящей публикации. IBM оставляет за собой право в любое время и без дополнительного уведомления исправлять и обновлять продукты и программы, упоминаемые в настоящей публикации.

Все встречающиеся в данной документации ссылки на Web-сайты других компаний предоставлены исключительно для удобства пользователей и не являются рекламой этих Web-сайтов. Материалы, размещенные на этих Web-сайтах, не являются частью информации по данному продукту IBM и ответственность за применение этих материалов лежит на пользователе.

IBM может использовать и распространять любую предоставленную вами информацию на свое усмотрение без каких-либо обязательств перед вами.

Для получения информации об этой программе для обеспечения: (i) обмена информацией между независимо созданными программами и другими программами (включая данную) и (ii) взаимного использования информации, полученной в ходе обмена, пользователи данной программы могут обращаться по адресу:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Такая информация может предоставляться на определенных условиях, включая, в некоторых случаях, уплату вознаграждения.

- | Описанная в этой информации лицензионная программа и все связанные с ней лицензионные материалы
- | предоставляются IBM в соответствии с условиями Соглашения с заказчиком IBM, Международного
- | соглашения о лицензии на программу IBM, Лицензионного соглашения о машинном коде IBM или любого
- | другого эквивалентного соглашения.

Все приведенные показатели производительности были получены в управляемой среде. В связи с этим результаты, полученные в реальной среде, могут существенно отличаться от приведенных. Некоторые измерения могли быть выполнены в системах, находящихся на этапе разработки, поэтому результаты измерений, полученные в серийных системах, могут отличаться от приведенных. Более того, некоторые значения могли быть получены в результате экстраполяции. Реальные результаты могут отличаться от указанных. Пользователи, работающие с этим документом, должны удостовериться, что используемые ими данные применимы в имеющейся среде.

Информация о продуктах других изготовителей получена от поставщиков этих продуктов, из их официальных сообщений и других общедоступных источников. IBM не выполняла тестирование этих продуктов других фирм и не может подтвердить точность заявленной информации об их производительности, совместимости и других свойствах. Запросы на получение дополнительной информации об этих продуктах должны направляться их поставщикам.

Все заявления, касающиеся намерений и планов IBM, могут изменяться и отзываться без предварительного уведомления, и отражают только текущие цели и задачи.

Все указанные здесь цены на продукты IBM - это рекомендованные IBM текущие розничные цены. Цены дилеров могут от них отличаться.

Эта информация предназначена только для планирования. Она может измениться прежде, чем описанный продукт станет доступен.

В этой публикации содержатся примеры использования данных и отчетов в повседневных деловых операциях. Для максимальной наглядности они снабжены именами людей, названиями компаний, товаров и продуктов. Все эти имена вымышлены, любое возможное сходство с названиями и адресами реальных предприятий является случайным.

Информация об авторских правах.

В этой публикации приведены примеры исходных текстов программ, иллюстрирующие приемы программирования для различных платформ. Вы можете копировать, изменять и распространять эти примеры бесплатно в целях разработки, использования, продажи и распространения программ, отвечающих спецификациям интерфейсов прикладного программирования для соответствующих платформ. Эти примеры не подвергались полному и всестороннему тестированию. По этой причине, IBM не может гарантировать, ни прямо, ни косвенно, их правильной работы, надежности и удобства в использовании.

В электронной версии данной документации фотографии и цветные иллюстрации могут отсутствовать.

Товарные знаки

Ниже перечислены товарные знаки International Business Machines Corporation в США и/или других странах:

- | AS/400
 - | DB2
 - | Domino
 - | Enterprise Storage Server
 - | eServer
 - | FlashCopy
 - | i5/OS
 - | IBM
 - | iSeries
 - | Lotus
 - | QuickPlace
 - | Redbooks
 - | Tivoli
 - | TotalStorage
- | Intel, Intel Inside (эмблемы), MMX и Pentium являются товарными знаками корпорации Intel в Соединенных Штатах и/или других странах.

Microsoft, Windows, Windows NT и эмблема Windows являются товарными знаками корпорации Microsoft в Соединенных Штатах и/или других странах.

Java, а также все товарные знаки, содержащие слово Java, являются товарными знаками корпорации Sun, Inc. в США и/или других странах.

- | Linux является товарным знаком Linus Torvalds в США и/или других странах.

UNIX является зарегистрированным товарным знаком Open Group в США и/или других странах.

Названия других компаний продуктов и услуг могут быть товарными или служебными знаками других компаний.

Условия

Разрешение на использование данных публикаций предоставляется на следующих условиях.

Использование в личных целях: Разрешается воспроизведение этих публикаций для личного, некоммерческого использования при условии сохранения в ней всех заявлений об авторских правах. Запрещается распространение, демонстрация и использование этих материалов в качестве основы для последующих публикаций, полностью или частично, без явного согласия на то фирмы IBM.

Использование в коммерческих целях: Разрешается воспроизведение, распространение и демонстрация этих публикаций исключительно в пределах предприятия при условии сохранения в ней всех заявлений об авторских правах. Запрещается использование этих публикаций в качестве основы для последующих произведений, а также воспроизведение, распространение и демонстрация этих публикаций, полностью или частично, за пределами предприятия без явного согласия на то фирмы IBM.

За исключением явно оговоренных в данном разрешении случаев, на публикацию и любую содержащуюся в ней информацию, данные, программное обеспечение и другие объекты интеллектуальной собственности не предоставляются никакие разрешения, лицензии и права, ни явные, ни подразумеваемые.

Фирма IBM оставляет за собой право в любой момент по своему усмотрению аннулировать предоставленные настоящим разрешением права, если сочтет, что использование этих публикаций наносит ущерб ее интересам или что указанные инструкции не соблюдаются должным образом.

Вы можете загружать, экспортировать и реэкспортировать эту информацию только в полном соответствии со всеми применимыми законами и правилами, включая все законы США в отношении экспорта.

IBM не дает никаких гарантий относительно содержания этих публикаций. Публикации предоставляются на условиях "как есть", без каких-либо явных или подразумеваемых гарантий, включая, но не ограничиваясь этим, подразумеваемые гарантии коммерческой ценности, соблюдения авторских прав или пригодности для каких-либо конкретных целей.



Напечатано в Дании